

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平10-21305

(43)公開日 平成10年(1998)1月23日

(51)Int.Cl. ⁶	識別記号	庁内整理番号	FI	技術表示箇所
G 0 6 F 17/60			G 0 6 F 15/21	3 3 0
G 0 6 T 7/00			H 0 4 M 3/42	Z
H 0 4 M 3/42			G 0 6 F 15/21	3 4 0 B
			15/62	4 6 5 U

審査請求 未請求 請求項の数2 FD (全 9 頁)

(21)出願番号 特願平8-188055

(22)出願日 平成8年(1996)7月1日

(71)出願人 000005810

日立マクセル株式会社

大阪府茨木市丑寅1丁目1番88号

(72)発明者 中村 昂

大阪府茨木市丑寅一丁目1番88号 日立マ
クセル株式会社内

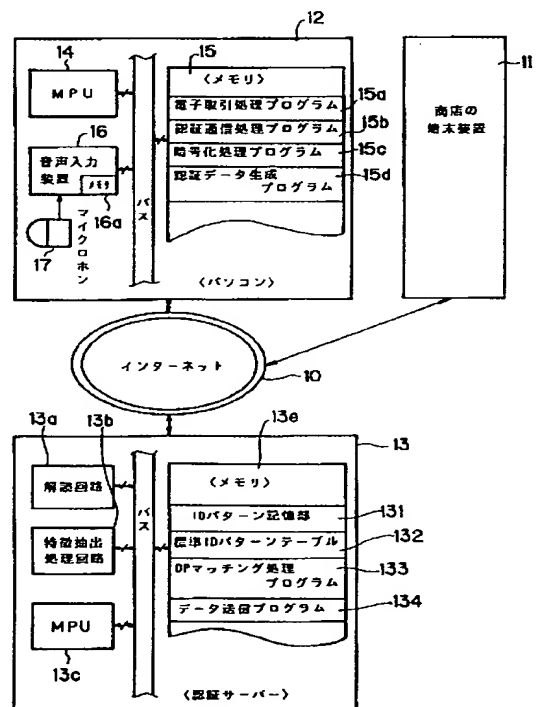
(74)代理人 弁理士 梶山 信是 (外1名)

(54)【発明の名称】 電子商品取引システム

(57)【要約】 (修正有)

【課題】より安全性の高い本人確認ができる電子商品取引システムを提供する。

【解決手段】インターネット10に接続され、商品購入の情報を受信する商店の端末装置11と、商品の購入者固有の身体的特徴の情報とこれを検索するための検索コードとを商品購入の情報に付加して認証サーバ13に送信する情報処理装置12とからなる。認証サーバ13は購入者固有の身体的特徴の情報を被照合情報として検索コードに対応させて記憶しているメモリ13eを有し、情報処理装置12から送出された身体的特徴と検索コードと商品購入の情報とを受けて検索コードにより検索した身体的特徴の情報との一致の有無を判定して、それらが一致しているときに、商店の端末装置11に商品購入についての情報を送出する。



【特許請求の範囲】

【請求項 1】ネットワークに接続された情報処理装置を利用して商品の売買を行う電子商品取引システムにおいて、

前記ネットワークに接続され、前記商品の販売情報を前記ネットワークを介して送出し、所定の商品購入についての情報を受信する第 1 の情報処理装置と、

前記ネットワークに接続され、前記商品の販売情報を受信して前記商品の購入の処理を行いつつ購入者固有の身体的特徴の情報とこれを検索するための検索コードとを前記商品購入についての情報に付加して特定の認証装置に送信する第 2 の情報処理装置と、

前記特定の認証装置として前記ネットワークに接続され、多数の購入者固有の身体的特徴の情報を被照合情報としてそれぞれに対応する検索コードにより検索できる状態で記憶している記憶媒体を有し、前記第 2 の情報処理装置から送出された身体的特徴の情報と前記検索コードと前記商品購入についての情報とを受けて受けた検索コードにより前記記録媒体を検索して得られる被照合情報と前記受信した身体的特徴の情報との一致の有無を判定してそれらが一致しているときに、前記第 1 の情報処理装置に前記商品購入についての情報を送出する第 3 の情報処理装置とを備える電子商品取引システム。

【請求項 2】前記ネットワークはインターネットであり、前記第 3 の情報処理装置は、前記記憶媒体に前記商品を取り扱う商品取扱者固有の身体的特徴の情報を被照合情報としてこれの検索コードとともにさらに有していて、前記第 2 の情報処理装置から前記受信した身体的特徴の情報との一致の有無を判定してそれらが一致しているときに、前記第 1 の情報処理装置に対して前記商品取扱者の身体的特徴の情報と前記この検索コードとの送信を要求し、前記第 1 の情報処理装置から送出された身体的特徴の情報と前記第 1 の情報処理装置から送出された前記検索コードとを受けて受けた検索コードにより前記記録媒体を検索して得られる被照合情報と前記受信した身体的特徴の情報との一致の有無を判定してそれらが一致しているときに、前記第 1 の情報処理装置に前記商品購入についての情報を送出し、少なくとも前記第 2 の情報処理装置から前記第 3 の情報処理装置における伝送データが暗号化されている請求項 1 記載の電子商品取引システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、電子商品取引システムに関し、詳しくは、インターネット等の公衆回線を介してコンピュータを利用して商品の購入を行い、個人認証をして代金の決済を行う電子商品取引システムにおいて、信頼性の高い本人認証を行うことができるような電子商品取引システムに関する。

【0002】

【従来の技術】電子商品取引システムの 1 つとして、デスクトップ型やノート型のパーソナルコンピュータ（以下パソコン）等を使用してインターネットに接続し、インターネット経由で所定のサービス会社のホームページに接続し、ホームページのサービス項目から、例えば、レストランの予約を選択し、日時、人数、料理コースなどを入力することでレストランの予約をするシステムがある。さらに、このような予約のほか、宿泊施設の予約、そして商品の購入も同様に特定の会社のホームページを閲覧してそのサービス項目から順次選択することで行われ、商品については、特定の商品が映像化され、画面上に表示された商品を選択し、選択した商品について商品番号、単価、数量等を入力して購入することが行われている。しかも、最近では、このような購入がパソコンを越えて PDA（携帯用情報通信端末）やこれに接続された簡易型携帯電話（PHS）などを使用する電子取引システムも提案されている。

【0003】このような電子商品取引システムにおいては、代金の決済に応じて、通常、クレジット会社や銀行から個人認証した個人や法人の口座から商品代金が引き落とされ、支払いが行われる。そこで、重要になるのは、購入者あるいは予約者の本人認証である。従来のこの種の認証には、ICカードが用いられ、これによる個人認証が行われて決済がなされる。特に最近では、前記の商品取引に応じて即座に決済が行われるオンライン決済も提案されている。インターネットを利用するのオンライン決済の 1 つとして、例えば、ICカード等を利用してインターネット上の接続会員のデータ管理を行うプロバイダの認証サーバーに送って、これにより個人認証をし、さらに前記の IC カードにより認証サーバーと IC カードとの確認情報をクレジット会社あるいは販売管理会社に設けられたサーバーに送って、これによりさらに認証確認をするという二重の確認処理により安全性の高い認証を行うシステムが提案されている。

【0004】図 6 は、予約販売会社とプロバイダーとの二重確認についての説明図である。まず、インターネット 10 上で接続された予約販売会社のサーバー 1 とパソコン 2 とが接続されて予約商品の選択が終了すると、パソコン 2 に IC カード 3 を装着して暗唱コードを入力する。IC カード 3 の情報と暗唱コードとが照合されるとともに、インターネット 10 を介してプロバイダの認証サーバー 4 に送出されてここでも個人認証が行われ、IC カード 3 に返される。このとき、認証サーバー 4 からパソコン 2 に本人であることとブラックリストとの照合結果などの所定の確認データが送出され、パソコン 2 に転送される。次に、パソコン 2 上の所定のキーを入力すると、インターネット 10 を介してパソコン 2 が予約サーバー 1 に対して認証サーバー 4 と IC カード 3 とによる交信結果データと予約情報と暗唱コード等が送出される。予約サーバー 1 に送信されたそれぞれの情報につ

いてさらに IC カード 3 との間で確認処理がなされた上で、予約処理が実行される。その結果、双方のサーバーで確認が採れたときに、クレジット会社 5 に金額決済のデータを送出し、会員の口座から代金が引き落とされる。もちろん、このとき、IC カード 3 の情報、暗唱コード、個人確認結果のデータ等は所定のスクランブル処理（あるいは暗号化処理）がなされ、これらのデータを受信した側はスクランブルの解除（あるいは解読処理）をすることになる。

【0005】

【発明が解決しようとする課題】電子商品取引システムは、このような特定のサービス会社を通す予約の場合ばかりでなく、個人商店や大小各種の会社がインターネット上でホームページを設けて、仮想商店により、商品の販売を行い、自由に販売商品の選択ができるようになっている。このような商店に対してそれぞれ予約サーバーに対応するような大きなシステムを設けることはできない。だからと言って、プロバイダによる認証だけでは安全性が低い。また、前記の個人認証は、IC カードによるものであり、単に個別の認証処理を認証サーバー 2 つにより重ねているものであって、二重の認証といっても、それぞれのサーバーが個別に入力された暗唱コードと IC カードからのデータに基づいて個人認証を行うシステムであることには変わりがない。しかも、暗唱コードは、操作中に盗み見られたり、生年月日などから容易に推定されて危険性が高く、IC カートの特定のコードは、データ量が少ないので、インターネット上を流れるときにハッカにより解読されてしまう危険性が高い。IC カードのシステムが解読されてしまえば、二重化した意味もなくなる。したがって、インターネット等の公衆に解放されたネットワークにおいて金額決済を含む電子商品取引システムでは、より安全性の高い本人確認が必要である。この発明は、このような従来技術の問題点に鑑みなされたものであり、より安全性の高い本人確認ができる電子商品取引システムを提供することを目的とする。

【0006】

【課題を解決するための手段】このような目的を達成するためのこの発明の電子商品取引システムの特徴は、ネットワークに接続された情報処理装置を利用して商品の売買を行う電子商品取引システムにおいて、ネットワークに接続され、商品の販売情報をネットワークを介して送出し、所定の商品購入についての情報を受信する第 1 の情報処理装置と、ネットワークに接続され、商品の販売情報を受信して商品の購入の処理を行いつつ購入者固有の身体的特徴の情報とこれを検索するための検索コードとを商品購入についての情報に付加して特定の認証装置に送信する第 2 の情報処理装置と、特定の認証装置として前記ネットワークに接続され、多数の購入者固有の身体的特徴の情報を被照合情報としてそれぞれに対応す

る検索コードにより検索できる状態で記憶している記憶媒体を有し、第 2 の情報処理装置から送出された身体的特徴の情報と検索コードと商品購入についての情報とを受けて受けた検索コードにより記録媒体を検索して得られる被照合情報と受信した身体的特徴の情報との一致の有無を判定してそれらが一致しているときに、第 1 の情報処理装置に商品購入についての情報を送出する第 3 の情報処理装置とを備えるものである。

【0007】

10 【発明の実施の形態】前記のように、この発明にあつては、本人確認のために、暗唱コードなどのパスワードを用いずに身体的特徴を用いることで、認証のためのデータ量が多くなる。それだけ認証データの解読がし難くなる。また、身体的特徴である関係からその人特有の情報になる。さらに、認証サーバー等の第 3 の情報処理装置に第三者機関として配置し、身体的特徴の情報を認証情報として商品購入情報と合わせて伝送するようにしている。このようにすることで、商品取引と本人確認とが第三者機関を介して行われることになるので信頼性が増加する。特に、身体的特徴の情報と検索コードの伝送情報は、第 2 の情報処理装置（商品購入者）から第 3 の情報処理装置（認証サーバー）と一方的に流れる伝送になっていて、さらに、購入情報も第 3 の情報処理装置（認証サーバー）から第 1 の情報処理装置と一方的に流れる伝送である。したがって、商品購入者と認証サーバーとの間だけで特殊な暗号化によりデータ送信ができる。また、商品の販売者（商品取扱者）と認証サーバーとの間でも必要な場合には別な暗号化も可能であり、ここでは購入者の身体的特徴の情報や検索コードの情報伝送は不要になる。その結果、IC カードのように、第 1 の情報処理装置と第 2 の情報処理装置あるいは第 3 の情報処理装置と第 2 の情報処理装置との間で個人確認されたことについてのデータの授受をしなくても済むので、信頼性が向上する。さらに、前記の一方向の伝送により購入者と商店との直接的な接続が関係が切り離されるので、誰がどの商品をどの商店から購入するのか、その関係が分かり難くなる。それだけ情報の解読がし難くなるので、商品取引に対する信頼性が向上する。また、専用に第 3 の情報処理装置を認証のために設けているので、IC カードに比べて確認データを大きな情報量で扱うことができ、例えば、声紋や、角膜紋、指紋、指の骨形状、顔面パターンなどをより解読が難しい確認データを利用することもできる。特に、第 3 の情報処理装置（認証サーバー）から第 1 の情報処理装置（商店側）に対しても同じように身体的特徴の情報と検索コードの伝送を要求して第 3 の情報処理装置で確認してから購入情報を第 1 の情報処理装置に送出するにすれば、購入者側の安全性も保証される。

【0008】

50 【実施例 1】図 1 は、この発明の電子商品取引システム

のインターネットを利用した一実施例のブロック図であり、図2は、電子取引処理の購入者側装置の処理のフローチャート、図3は、電子取引における商品購入フォーマットの一例の説明図、図4は、電子取引処理における認証サーバーの処理のフローチャート、そして、図5は、インターネットを利用した電子商品取引システムの全体的な構成図である。なお、図6に示すものと同一の構成要素は同一の符号で示す。図5において、11は、インターネット10に接続されたインターネットに接続されるホームページを有するある商品を販売するある商店の端末装置（仮想商店）であり、12は、商店の端末装置11からある商品を購入するインターネット10に接続された個人のパソコンである。13は、インターネット10に接続された認証サービス会社の認証サーバーである。なお、6は、インターネットとの接続を管理しているプロバイダである。認証サーバー13は、特定のプロバイダ6とは関係なしに、商店の端末装置11や個人のパソコン12と同様に第三者として単にインターネット10に接続されているものである。

【0009】ここで、パソコン12には、図1に示されるように、MPU14とメモリ15、そして、音声入力装置16、マイクロホン17等を有している。音声入力装置は、IDとなる音声を入力するものであって、マイクロホン17からピックアップされた音声を所定の周波数 f_0 でサンプリングしてA/D変換し、デジタル値のビットデータを生成してその内部メモリ16aに記憶する。メモリ15には、電子取引処理プログラム15a、認証サーバー13に対する認証通信処理プログラム15bと暗号化処理プログラム15c、そして、認証データ生成プログラム15d等が設けられている。なお、商店の端末装置11は、いわゆる商品取扱者が操作するコンピュータであって、前記のパソコン2と同様なプログラムと構成を有しているが、ここでは、その内部は省略してある。認証サーバー13は、送信されたデータをあらかじめ取決めである個人ごとの暗号キーで元のデータに復元する解読回路13aと、送信された音声IDのデータから特徴抽出処理をする特徴抽出処理回路13bと、MPU13c、そしてメモリ13eとを有している。メモリ13eには、伝送された音声IDの抽出された特徴パターンを記憶する音声IDパターン記憶部131、そして、標準IDパターンテーブル132、DPマッチング処理プログラム133、データ送信プログラム134等を有している。なお、標準IDパターンテーブル132は、多数の検索コードに対応してそれぞれの音声IDの標準パターンを記憶するものであって、送信された暗号キーに対応する標準音声IDパターンを検索するテーブルである。このテーブルは、DPマッチング処理プログラム133により検索され、検索されて得られた標準パターンの1つと音声IDパターン記憶部131のパターンデータとがDP法によってマッチング処理

されて、これらの一致、不一致が判定される。

【0010】MPU14は、所定の条件が成立したときに電子取引処理プログラム15aを実行する。電子取引処理プログラム15aは、これが実行されると、前記の各プログラムを順次コールしてMPU14に実行させていく。図2に従って、その処理を説明すると、電子取引処理プログラム15aは、個人がパソコン12を介してインターネットの接続状態に入り、商店の端末装置11のホームページに接続して、これから商品選択項目が選択されて図3の(a)に示すようなフォーマットで、商品購入情報7がインターネット10を介してパソコン12の画面上に得られたとする。この場合に、暗号キー入力欄60にカーソルが位置付けられ、あるいはマウスにより指定が行われたときに割り込みスタートをする。なお、図3の(a)において、50は販売元アドレス欄、51はプロバイダ等の伝送情報欄、52は商品番号欄、53は数量/単価欄、54は購入金額欄、55は商品画像表示欄、56は発送先住所欄/発送先コード欄、57は氏名、電話番号等の連絡先欄、58は届日時希望欄、59はその他情報欄、60は暗号キー入力欄、そして61は音声ID入力欄である。

【0011】MPU14は、まず、商品購入情報7のうち欄59までの入力が済んだ時点で、カーソルあるいはマウスにより暗号キー入力欄60が指定されると、電子取引処理プログラム15aをコールして実行する。電子取引処理プログラム15aの実行によりMPU14は、まず、販売元アドレス欄50の情報に加えて、入力された商品番号、数量、発送先住所等の欄59までの購入情報を含めた商品購入情報7を抽出し、メモリ15の所定の領域あるいはハードディスクの所定の領域に退避させて記憶する（ステップ101）。その後、認証データ生成プログラム15dをコールする。MPU14は、認証データ生成プログラム15dを実行して、まず、暗唱コード入力メッセージ等を表示してコード自体を欄60には表示しないように処理して暗唱コードの入力を操作者にさせ（ステップ102）、これの入力後に続いて欄61にカーソルをシフトさせて同様に内容表示をせずに音声ID入力をさせる（ステップ103）。これにより操作者が音声IDとして、例えば、マイクロホン17から「山川鳥花」という音声の入力が終了すると、キーボードのリターンキーが待ちループに入り（ステップ104）、キーボードからリターンキーが入力されると、MPU14は、音声入力装置16のメモリ16aからデジタル値に変換された音声IDデータを取込み（ステップ105）、前記の暗号キーとともにメモリ13の所定の領域に記憶する（ステップ106）。

【0012】認証データ生成プログラム15dの処理が終了すると、電子取引処理プログラム15aは、暗号化処理プログラム15cをコールして前記の音声IDの「山川鳥花」を暗唱コードで暗号化したデータを生成

し、メモリ 1 3 に記憶し（ステップ 1 0 7）、さらに前記の商品購入情報 7 を暗号キーで暗号化したデータを生成し、メモリ 1 3 あるいはハードディスクに記憶する（ステップ 1 0 8）。なお、このとき、暗号化した各データを圧縮処理をしてもよい。次に、暗号化処理プログラム 1 5 c の処理が終了すると、電子取引処理プログラム 1 5 a は、認証通信処理プログラム 1 5 b をコールする。MPU 1 4 は、認証通信処理プログラム 1 5 b を実行することで、送信先に認証サーバー 1 3 を指定して図 3 の（b）のフォーマット 1 8 の電文を作成して（ステップ 1 0 9）、認証サーバー 1 3 に対するメールとしてインターネット 1 0 に送出する（ステップ 1 1 0）。なお、（b）においては、まず、送信相手先アドレス 1 8 a として認証サーバー 1 3 のアドレスを挿入し、その後販売元アドレス 1 8 b、販売元認証フラグ 1 8 c、発信元アドレス 1 8 d、暗唱コード 1 8 e、音声 ID データ 1 8 f、DLE（データリンクエスケープコード） 1 8 g、SYN（同期コード） 1 8 h、そして、先にハードディスクに退避してある商品購入情報 1 8 i が送出される。なお、暗唱コード 1 8 d は、このとき所定の関数でスクランブル処理されたものであってもよい。

【0013】一方、認証サーバー 1 3 は、図 4 に示すように、受信割り込みスタートで処理を開始し、MPU 1 3 c の受信処理により、図 3 の（b）のフォーマット 1 8 の電文を受信すると（ステップ 2 0 1）、この受信データからまず、暗号キー 1 8 a を抽出（スクランブル処理されているときにはスクランブルを解除）する（ステップ 2 0 2）。なお、データ圧縮されているときには圧縮解凍をする。そして、暗唱コード 1 8 a をキーとして解読回路 1 3 a に受信データを転送して、これにより送信された受信データを復元する（ステップ 2 0 3）。MPU 1 3 c は、次に復元データから音声 ID データ 1 8 c の部分を抽出して特徴抽出処理回路 1 3 b に転送する（ステップ 2 0 4）。そして、特徴抽出処理回路 1 3 b において転送された音声 ID の特徴パターンが抽出され、この特徴パターンを特徴抽出処理回路 1 3 b から取込み（ステップ 2 0 5）、それを受けて MPU 1 3 c は、音声 ID パターン記憶部 1 3 1 に記憶する（ステップ 2 0 6）。次に、MPU 1 3 c は、DP マッチング処理プログラム 1 3 3 を実行して、音声認証処理として、暗唱コードにより標準 ID パターンテーブル 1 3 2 を検索して暗号キーに対応する標準パターンを読み出して（ステップ 2 0 7）、そして、これと音声 ID パターン記憶部 1 3 1 のデータとを DP 法により音声マッチング判定をする（ステップ 2 0 8）。

【0014】このマッチング判定で音声 ID が一致すると判定されたときには、MPU 1 3 c は、受信データの販売元認証フラグ 1 8 c を参照してここにフラグが立っているか否かを判定し（通常はフラグを立てるものとする）、これにより商店の端末装置 1 1 について認証す

るか否かの判定をする（ステップ 2 0 9）。最初は、ここで YES となり、前記の認証フラグをリセットして（ステップ 2 1 0）、受信データの販売元アドレス 1 8 b を抽出して（ステップ 2 1 1）、商店の端末装置 1 1 に対して注文ありの電文とともに所定のフォーマットに従って音声 ID と暗唱コードの入力をして送信することを促すメッセージの電文を伝送を送出する（ステップ 2 1 2）。そして、受信待ちにループに入る（ステップ 2 1 2）。これにより商品取扱者の音声 ID による認証処理を行う。なお、受信データの販売元認証フラグ 1 8 c がリセットされた状態で受信したときには、前記のステップ 2 0 9 の判定で NO となるので、後述するステップ 2 1 4 において認証サーバー 1 3 が商店の端末装置 1 1 に商品購入情報 7 を送出することになる。購入者はこの販売元認証フラグをリセットする選択ができるものとする。さて、商店の端末装置 1 1 から音声 ID と暗唱コードを受けると、この音声 ID と暗唱コードについて認証をするために前記のステップ 2 0 1 へと戻り、ステップ 2 0 1 からステップ 2 0 7 を経て、ステップ 2 0 8 の判定で音声 ID が一致しているとされたときには、今度は、ステップ 2 0 9 の認証フラグ判定で NO となる。そこで、入力された商品番号、数量、送り先アドレス等の購入情報を含めた商品購入情報 7 が発信元を認証サーバー 1 3 としてインターネット 1 0 を介して商店の端末装置 1 1 に送出する（ステップ 2 1 4）。なお、音声マッチング判定で不一致のときには、発信元アドレス 1 8 d に従ってアクセス拒否、再送要求応答が発信元に送出される（ステップ 2 1 5）。

【0015】このようにすることで、商店の端末装置 1 1 は、発信元が認証サーバー 1 3 であるときには、個人認証が完了しているものとして、商品を安心して発送できる。また、認証サーバー 1 3 は、このとき、商店の端末装置 1 1 と購入者との間に第三者として介在し、かつ、音声 ID という個人特有の特徴により認証を行うので、安全性の高い照合ができる。その結果、電子商品取引システムの信頼性を向上させることができ、さらに、認証サーバー 1 3 から音声 ID 認証を行った個人のデータと送信されたデータから金額等を抽出して暗唱コードとともにクレジット会社へ送信して金額引き落としの決済の送信をして即座にオンライン決済することができる。

【0016】ところで、この実施例のように専用の認証サーバーを設けることで、認証情報のデータ量は、IC カードよりも多くの容量を割り当てることができる。これにより、秘密性を向上させ、データの信頼性を高めることができる。そこで、各商店の端末装置 1 1 やパソコン 1 2 に備える認証のための入力装置としては、操作者の身体的特徴として、音声 ID ばかりではなく、例えば、声紋入力手段により声紋を入力し、認証サーバー 1 3 により声紋を比較判定するようにしてもよい。すなわ

ち、入力された声紋は、暗号化手段によって暗号化された後に、一般のネットワーク経路で認証サーバー13に転送される。認証サーバー13は、受信した暗号化声紋を復号化手段で復号化して入力声紋情報を得る。そして、同時に受信した操作者の暗号コード（操作者のID）に基づいて照合手段を用いて登録済みの声紋ファイルから当該操作者の声紋を抽出して入力声紋と比較照合し、合致したら本人と見なす処理をする。なお、一般のネットワークを利用してデータを送信する関係での暗号化としては、前記の暗号コードによるもののほかに、操

作者ごとに予め設定した、例えば、秘密キー、可変キーなども加えて暗号処理をして、これらのキーとともに伝送情報を認証サーバー13に送信するようにしてもよい。

【0017】この場合には、認証サーバー13は、送信された秘密キー、可変キーなどを解読キーとして利用する。例えば、声紋等の復号化にあたっては秘密キーに対応した公開キーを公開キーファイルから暗号コードに基づいて抽出して用いることができる。可変キーとして

は、例えば、日時など、暗号結果を毎回異ならせて、送信中に仮に盗まれても、毎回結果が異なるようにして、単純に複製しても不正利用できないようにすることができる。

【0018】以上説明してきたが、実施例では、購入者のパソコンと商品取扱者（販売者）の端末装置とは直接データの授受を行う接続がなされることはなく、データが相互伝送されることはない。商品の購入のときには、認証サーバーが介在して購入情報のデータが商品取扱者に伝送される。また、商品購入の際にも購入者のパソコンは、認証が正しいときには、単に認証サーバーにデータを送信するだけになる。また、ネットワークに接続される装置は、パソコンのみならず電話機や携帯電話機やPHSやPDAやインターネットTVなどであってもよい。また、電子化された身体的特徴は、声紋のみならず角膜紋、指紋、指の骨形状、顔面パターンなど、個人の

特徴を識別できるものであればよい。さらに、ネットワークは、有線、無線を問わずまた電話網、通信回線、CATV、衛星通信などでもよい。暗号化手段や復号化手段は公開鍵方式、秘密鍵方式のいずれでもよい。

【0019】

【発明の効果】この発明にあつては、暗唱コードなどのパスワードを用いずに身体的特徴を用いることで、認証のためのデータ量が多くなる。それだけ認証データの解読がし難くなり、また、身体的特徴である関係からその人特有の情報になる。さらに、認証サーバー等の第3の情報処理装置に第三者機関として配置し、身体的特徴の情報を認証情報として商品購入情報と合わせて伝送するようにしているので、商品取引と本人確認とが第三者機関を介在して行われることになるので信頼性が増加す

る。特に、身体的特徴の情報と検索コードの伝送情報は、第2の情報処理装置（商品購入者）から第3の情報処理装置（認証サーバー）と一方的に流れる伝送になっていて、さらに、購入情報も認証サーバーから第1の情報処理装置（商品取扱者）と一方的に流れる伝送であるので、商品購入者と認証サーバーとの間だけで特殊な暗号化によりデータ送信ができる。また、商品の販売者（商品取扱者）と認証サーバーとの間でも必要な場合には別な暗号化も可能であり、ここでは購入者の身体的特徴の情報や検索コードの情報伝送は不要になる。また、ICカードのように、第1の情報処理装置と第2の情報処理装置あるいは第3の情報処理装置と第2の情報処理装置との間で個人確認されたことについてのデータの授受をしなくても済むので、信頼性が向上する。その結果、従来のICカード等を利用したパスワード方式に比べ大幅な機密の向上を図ることができる。さらに、身体的特徴の照合を操作手段側にて行わないずに、第三者の認証サーバー等の第3の情報処理装置で行うことにより、インターネットなどのような利用相手を限定できないオープンな公衆ネットワークにおいて信頼性の高い電子商品取引を行うことができる。

【図面の簡単な説明】

【図1】図1は、この発明の電子商品取引システムのインターネットを利用した一実施例のブロック図である。

【図2】図2は、電子商品取引処理の購入者側装置の処理のフローチャートである。

【図3】図3は、電子取引における商品購入フォーマットの一例の説明図であつて、（a）は、その表示画面における入力フォーマットの説明図、（b）は、そのデータ伝送フォーマットの説明図である。

【図4】図4は、電子商品取引処理における認証サーバーの処理のフローチャートである。

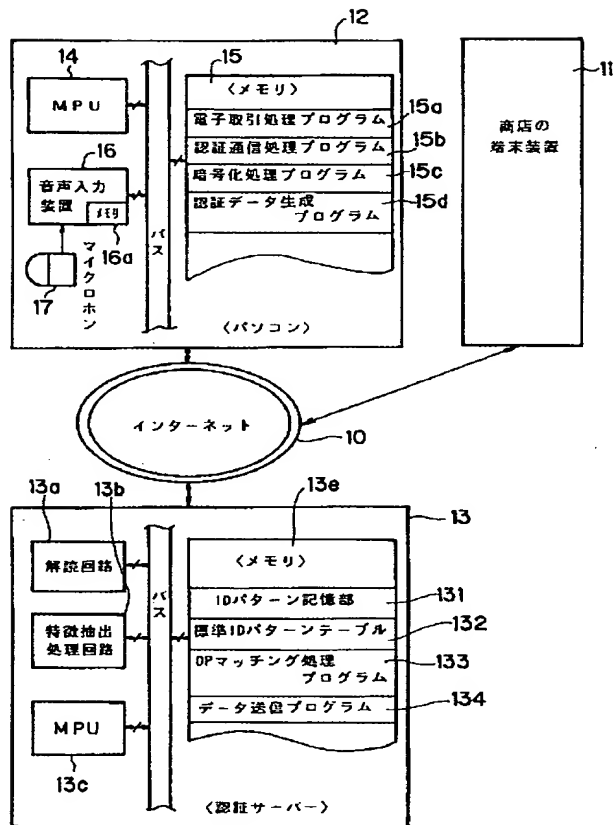
【図5】図5は、インターネットを利用した電子商品取引システムの全体的な構成図である。

【図6】図6は、インターネットを利用した従来の電子商品取引システムの説明図である。

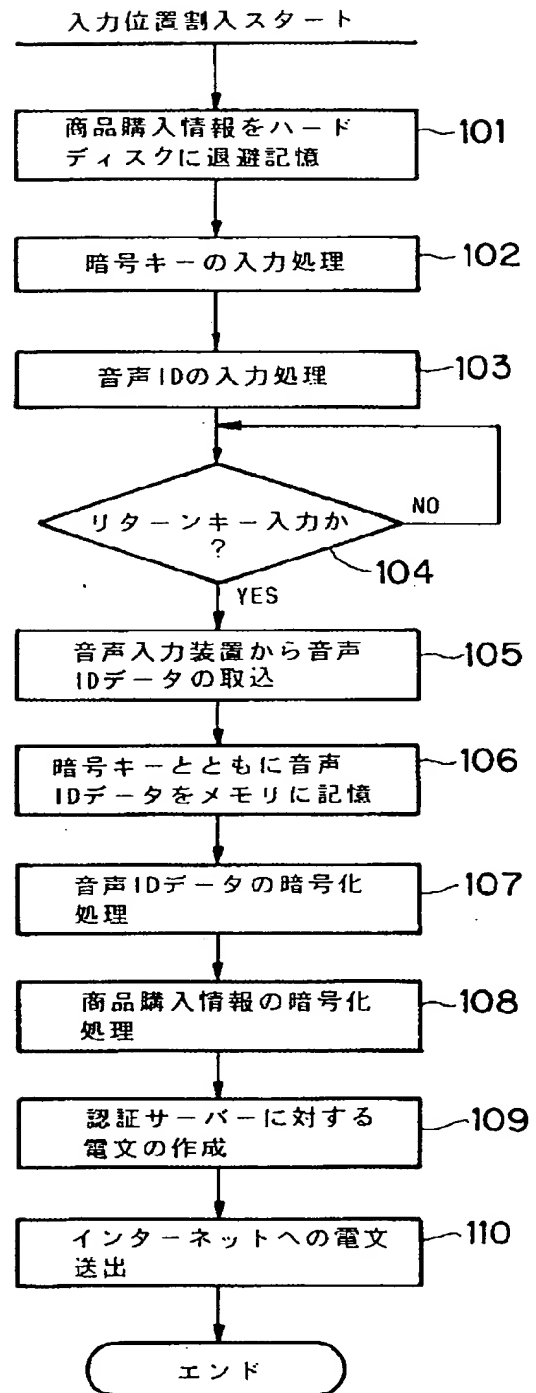
【符号の説明】

1…予約販売会社のサーバー、3…ICカード、10…インターネット、11…商店の端末装置、2、12…パーソナルコンピュータ（パソコン）、4、13…認証サーバー、13a…解読回路、13b…特徴抽出処理回路、13e、15…メモリ、131…音声IDパターン記憶部、132…標準IDパターンテーブル、133…DPマッチング処理プログラム、134…データ送信プログラム、13c、14…MPU、16…音声入力装置、17…マイクロホン、15a…電子取引処理プログラム、15b…認証通信処理プログラム、15c…暗号化処理プログラム、15d…認証データ生成プログラム。

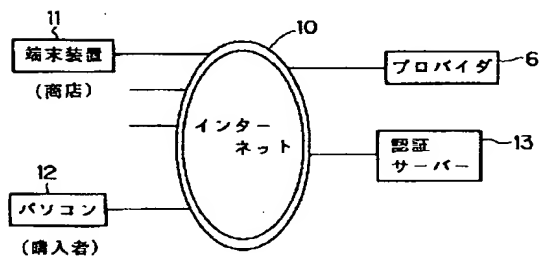
【図 1】



【図 2】



【図 5】

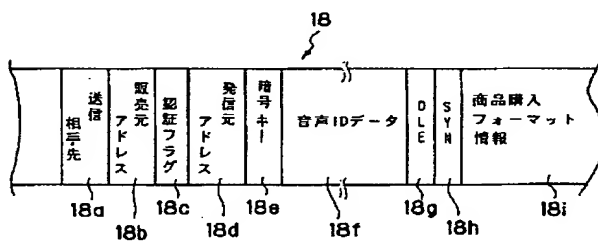


【図3】

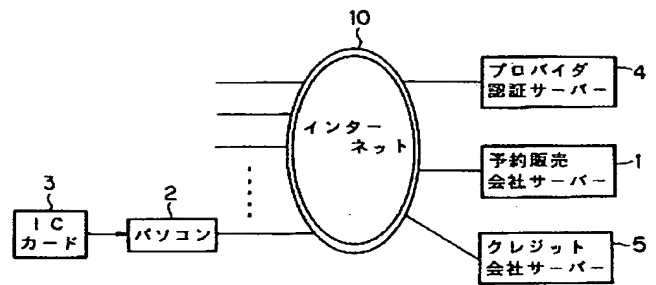
(a)

Form 7 is a rectangular form divided into two main sections. The left section, labeled 50, contains a vertical list of input fields: 51 (販売元アドレス), 52 (伝送情報), 53 (商品番号), 54 (数量/単価), 56 (購入金額), 57 (発送先住所), 58 (連絡先), 59 (展日時), and 59 (その他). The right section, labeled 55, is a large rectangular area containing a stylized bird logo. Below the logo are two small rectangular boxes labeled 60 and 61, each containing five asterisks (*****).

(b)



【図6】



【図4】

